REMARKS/ARGUMENTS

Favorable reconsideration of this application in light of the following remarks is respectfully requested.

Claims 1-3 and 6-26 are pending in the present application. No claims are added, amended, or canceled by the present response.

In the outstanding Official Action, Claims 1-9 and 11-18 were rejected under 35 U.S.C. § 102(e) as anticipated by European Patent Application EP 0982895 to Shimizu et al. (herein "Shimizu"); and Claim 10 was rejected under 35 U.S.C. § 103(a) as unpatentable over Shimizu in view of U.S. Patent No. 5,933,501 to Leppek.

Applicants respectfully traverse the rejection of Claims 1-9 and 11-18 under 35 U.S.C. § 102(e) as anticipated by Shimizu.

Applicants respectfully submit that Shimizu fails to teach or suggest each feature of the independent claims. Further, Applicants respectfully traverse the assertion in the Office Action that because the key conversion functions of Shimizu employ involution functions, Shimizu discloses the inverse relationships recited in the independent claims. However, Applicants respectfully submit that Shimizu fails to teach or suggest

> a first portion including at least two round processing circuits having first and second round functions and a second portion which follows the first portion, the second portion including at least two round processing circuits having third and fourth round functions, the third round function being an inverse of the second round function, and the fourth round function being an inverse of the first round function,

as recited in Claim 1, and as similarly recited in independent Claims 11, 13, and 15-18.

Shimizu merely describes a cryptographic data processor that includes "a plurality of key conversion functions fk sequentially connected, which each are an involution type" and "a plurality of round functions fr sequentially connected,

which are an involution type."[1] According to Shimizu, an involution function is a kind of bi-directional function, and the conversion and the reverse conversion of the function are the same.[2] Thus, Applicants respectfully submit that object of the present invention cannot be attained by the involution function, as described by Shimizu.

Further, Applicants respectfully traverse the assertion in the Office Action that Shimizu's indication that "a cipher text encrypted by an encryption key can be decrypted by a decryption key, while a cipher text encrypted by a decryption key can be decrypted by an encryption key (column 4, lines 11-22)" is interrupted as disclosing a common key which is output from the last stage of the key conversion functions.[3] However, the common key of the claimed inventions is a key that is input to the first stage and output from the last stage. The input key and the output key are the same in the present invention and they are called "common keys." On the other hand, according to Shimizu, it is not necessary for an encryption key and a decryption key to be same.[4]

Shimizu fails to teach or suggest that the encryption key and the decryption key must be the same. In order to make the encryption key equal to the decryption key, it would be necessary to impose a limitation on the round functions included in the expanded key scheduling section. However, Applicants respectfully submit that Shimizu fails to teach or suggest such a limitations. On the other hand, the claimed inventions use the same round processing circuits or the same portion of the round processing circuits of the expanded key scheduling section for an encryption circuit and the expanded key scheduling section for a decryption circuit.

---

[1] Shimizu at Abstract.
[2] Shimizu at column 8, lines 29-39.
[3] Office Action at page 3, lines 3-11.
[4] Shimizu at column 3, lines 32-33.

In order to output the same value as the input key, as the common key, it is necessary to have limitations such as those recited in the Claim 1. In particular, the round processing circuit comprises a first portion including at least two round processing circuits having first and second round functions and a second portion which follows the first portion, the second portion including at least two round processing circuits having third and fourth round functions, the third round function being an inverse of the second round function, and the fourth round function being an inverse of the first round function.

On the other hand, Shimizu fails to teach or suggest those limitations. A comparison between Shimizu and the claimed inventions is shown in an attached diagram, which provides support for the differences explained below.

In Shimizu, an encryption is expressed by

$$Y = F(X) = f_k \cdot f_{k-1} \cdot \ldots \cdot f_2 \cdot f_1 (X). \qquad (1)$$

and a decryption is expressed by

$$X = F^{-1}(Y) = f_1^{-1} \cdot f_2^{-1} \cdot \ldots \cdot f_{k-1}^{-1} \cdot f_k^{-1} (Y). \qquad (2)$$

If f is an involution type, i.e., $f_k^{-1} = f_k$, $f_{k-1}^{-1} = f_{k-1}$, ..., $f_2^{-1} = f_2$, ..., $f_1^{-1} = f_1$, Eq. 2 can be rewritten as

$$X = F^{-1}(Y) = f_1 \cdot f_2 \cdot \ldots \cdot f_{k-1} \cdot f_k (Y) \qquad (3)$$

Eq. 3 shows that the decryption is performed by the reverse order of the encryption. Thus, Shimizu indicates that extended keys are generated in a reverse order by using the involution functions in a reverse order.

However, in a process according to the claimed inventions, if the expanded key generating circuit comprises four round processing circuits, the encryption is expressed by

$$Y = F(X) = f_4 \cdot f_3 \cdot f_2 \cdot f_1(X) \qquad (4)$$

As recited in Claim 1, $f_4 = f_1^{-1}$ and $f_3 = f_2^{-1}$ so that $f_2^{-1} \cdot f_2 = 1$ and $f_1^{-1} \cdot f_1 = 1$. Thus, Eq. 4 can be rewritten as

$$Y = f_4 \cdot f_3 \cdot f_2 \cdot f_1(X) = f_1^{-1} \cdot f_2^{-1} \cdot f_2 \cdot f_1(X) = f_1^{-1} \cdot f_1(X) = X \quad (5)$$

Thus, in a process according to Claim 1, decryption may be expressed by

$$X = F^{-1}(Y) = f_1^{-1} \cdot f_2^{-1} \cdot f_3^{-1} \cdot f_4^{-1}(Y) = f_4 \cdot f_3 \cdot f_3^{-1} \cdot f_4^{-1}(Y) = f_4 \cdot f_4^{-1}(Y) = Y \quad (6)$$

Eqs. 5 and 6 show that, in the claimed approach, the input key and output key are the same.

Accordingly, Applicants respectfully submit that Shimizu fails to teach or suggest

> a first portion including at least two round processing circuits having first and second round functions and a second portion which follows the first portion, the second portion including at least two round processing circuits having third and fourth round functions, the third round function being an inverse of the second round function, and the fourth round function being an inverse of the first round function,

as recited in Claim 1, and as similarly recited in independent Claims 11, 13, and 15-18.

Thus, it is respectfully submitted that independent Claims 1, 11, 13, and 15-18, and claims depending therefrom, patentably define over Shimizu.

Further, Applicants respectfully traverse the rejection of Claim 10 under 35 U.S.C. § 103(a) as unpatentable over Shimizu in view of Leppek.

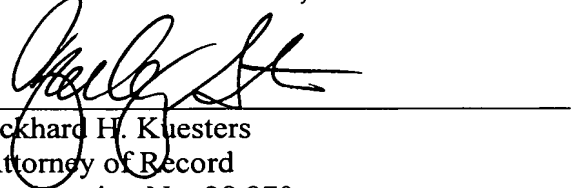
Claim 10 depends from Claim 1, which is believed to patentably define over Shimizu as discussed above. Further, Applicants respectfully submit that Leppek fails to teach or suggest the claimed features lacking in the disclosure of Shimizu. Thus, it is respectfully requested the rejection of Claim 10 under 35 U.S.C. § 103(a) be withdrawn.

Accordingly, Applicants respectfully submit that independent Claims 1, 11, 13, and 15-18, and claims depending therefrom, are allowable.

Consequently, in view of the present amendment and in light of the above discussion, no further issues are believed to be outstanding, and the present application is believed to be in condition for formal allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870

Zachary S. Stern
Registration No. 54,719

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

EHK:ZSS:pae

I:\ATTY\ZS\21's\211\211428US\211428 AM DUE 09-16-06.DOC